MATH 596: Quadratic and modular forms

notes by

Marcel K. Goh

10 December 2021

Disclaimer. These notes were taken for the class MATH 596, given at McGill University by Prof. Henri Darmon at McGill University during the Fall 2021 semester. Over the course of the term, students were asked to present solutions to exercises. I have indicated when this occurred by attaching students' names to their respective solutions. However, in some cases, the solution I recorded here is not word-for-word the one presented, as I sometimes found a modification that I understood better. An exercise solution that is unattributed does not necessarily indicate that it is completely my work, since I spent a lot of time discussing the material with my classmates. But any error that appears in the notes or exercise solutions, whether typographical or mathematical, are due to me and me alone.

Let V be a module over a commutative ring R. A function $Q : V \to R$ is a *quadratic form* if it satisfies

i) $Q(ax) = a^2Q(x)$ for all $a \in R$ and $x \in V$; and
ii) the function $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.

We call (V, Q) a *quadratic module*; if R is a field, V is a vector space and we call (V, Q) a *quadratic space* instead. When R is a field of characteristic not equal to 2, we can let

$$x \cdot y = \frac{1}{2}\bigl(Q(x + y) - Q(x) - Q(y)\bigr).$$

This defines a symmetric bilinear form on V, and we have $Q(x) = x \cdot x$ and there is a one-to-one correspondence between symmetric bilinear forms and quadratic forms (which is not true if the characteristic of the field is equal to 2).

Pick a basis $(e_i)_{i=1}^n$ of V. The matrix $A = (a_{ij})$ where $a_{ij} = e_i \cdot e_j$ is a symmetric matrix, and for $x = \sum_i^n x_ie_i \in V$,

$$Q(x) = \sum_{i=1}^n \sum_{j=1}^n a_{ij}x_ix_j.$$

If we switch to a new basis with the invertible change-of-basis matrix B, then the matrix of Q with respect to this new basis is the matrix BAB^{T}, which has determinant $\det(A)\det(B)^2$. We see then that for a quadratic form Q, the determinant of the matrix A corresponding to Q in any basis is unique up to multiplication by an element of $(k^\times)^2$; we call this the *discriminant* of Q and denote it by $\operatorname{disc} Q$.

Two elements x and y are *orthogonal* if $x \cdot y = 0$. For a subset $W \subseteq V$, we define a vector subspace

$$W^\perp = \{x \in V : x \cdot y = 0 \text{ for all } y \in W\}.$$

Two vector subspaces W_1 and W_2 of V are said to be *orthogonal* if $W_1 \subseteq {W_2}^\perp$ (this is a symmetric relation). We call $V^\perp$ the *radical* of V and say that V is *nondegenerate* if $V^\perp = \{0\}$. The codimension of $V^\perp$ is called the *rank* of V. If V is the direct sum of vector subspaces $W_1, \ldots, W_n$ and the W_i are pairwise orthogonal, then we say that V is the *orthogonal direct sum* of the W_i, and write

$$V = W_1 \mathbin{\widehat{\oplus}} \cdots \mathbin{\widehat{\oplus}} W_n.$$

An element $x \in V$ is said to be *isotropic* if $x \cdot x = 0$, and a subspace is *isotropic* if all of its elements are. If no nonzero element in a subspace W is isotropic, the W is said to be *anisotropic*. The linear span of two basis vectors e and f with $e \cdot e = f \cdot f = 0$ and $e \cdot f = 1$ is called a *hyperbolic plane* and is often denoted H.

Exercise 1. *Let V be a nondegenerate quadratic space. Show that any two maximal isotropic spaces of V have the same dimension, t, called the Witt index of V. Show that V is isomorphic to an orthogonal direct sum of t hyperbolic spaces and an anisotropic space W of dimension $n - 2t$ (where $n = \dim V$).*

Proof. (Hazem Hassan and Arihant Jain.) We start with the claim that any two maximal isotropic spaces have the same dimension. First observe that if U is a maximal isotropic subspace, then any $u \in U^\perp$ with $u \cdot u = 0$ must also be in U, otherwise we could extend U and contradict maximality. So let U_1 and U_2 be maximal isotropic subspaces. If $U_1 = U_2$ we are done; otherwise, consider $U_1 \times U_2 \to k$ that maps $(u_1, u_2) \mapsto u_1 \cdot u_2$. If u_1 is such that $u_1 \cdot u_2 = 0$ for all $u_2 \in U_2$, then by the observation above, $u_1 \in U_2$. So the left kernel of this map is $U_1 \cap U_2$ and a similar argument shows that this is also the right kernel. This means the map

$$\frac{U_1}{U_1 \cap U_2} \times \frac{U_2}{U_1 \cap U_2} \to k$$

is a perfect pairing; that is, $U_1/(U_1 \cap U_2) \to \operatorname{Hom}_k\bigl(U_2/(U_1 \cap U_2), k\bigr)$ is an isomorphism and vice versa. So $\dim U_1 = \dim U_2$.

Now we show that we can write $V = W \mathbin{\widehat{\oplus}} H_1 \mathbin{\widehat{\oplus}} \cdots \mathbin{\widehat{\oplus}} H_t$ where W is anisotropic, t is the dimension of every maximal isotropic subspace of V, and the H_i are hyperbolic spaces. Let $H_i = ke_i \oplus kf_i$ where $e_i \cdot e_i = 0 = f_i \cdot f_i$ and $e_i \cdot f_i = 1$. Let $U = ke_1 \oplus \cdots \oplus ke_t$. Then we see that U is isotropic, since $U^\perp = U \mathbin{\widehat{\oplus}} W$ and for $v = u + w$ in this space, $v \cdot v = (u + w) \cdot (u + w) = w \cdot w$ is only zero if $w = 0$. Hence U is maximal and isotropic, proving that every maximal isotropic subspace has dimension t. ∎

Quadratic spaces over R. Note that $\mathbf{R}^\times/(\mathbf{R}^\times)^2 = \{\mathbf{R}_{\geq 0}, \mathbf{R}_{\leq 0}\}$. If V is a nondegenerate quadratic space over $\mathbf{R}$, then it has an orthogonal basis

$$e_1, \ldots, e_r, e_{r+1}, \ldots, e_{r+s}$$

with $e_j \cdot e_j = 1$ for $1 \le j \le r$ and $e_j \cdot e_j = -1$ for $r+1 \le j \le r+s$. The pair (r, s) is called the *signature* of the quadratic space. The Witt index of V is $t = \min\{r, s\}$, and if $V = W \mathbin{\widehat{\oplus}} H^t$, where H^t is the orthogonal direct sum of h copies of a hyperbolic plane, then $\dim W = |r - s|$. When $r > s$, W is positive definite and when $r < s$, W is negative definite.

The orthogonal group $\mathrm{O}(V)$ of a quadratic space V over R is the space

$$\mathrm{O}(V) = \{g \in \mathrm{Aut}(V) : gv \cdot gw = v \cdot w \text{ for all } v, w \in V\}.$$

Letting $n = \dim V$ and (r, s) be the signature of the space, this can be viewed as the set of $n \times n$ matrices

$$\left\{A \in \mathrm{M}_n(\mathbf{R}) : A^{\mathrm{T}}A = AA^{\mathrm{T}} = \begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}\right\},$$

where the I_r and I_s that appear in the block matrix are the $r \times r$ and $s \times s$ identity matrices, respectively. The condition implies that $\det(A)^2 = 1$, meaning that $\det A = \pm 1$ for all $A \in \mathrm{O}(V)$. The subgroup of $A \in \mathrm{O}(V)$ with $\det(A) = 1$ is called $\mathrm{SO}(V)$. It was proven in class by a standard inductive argument that $\mathrm{O}(V)$ is a real manifold (and thus a *Lie group*) of dimension $n(n-1)/2$, and so is the subgroup $\mathrm{SO}(V)$.

Hamilton quaternions. The *Hamilton quaternions* are members of the set $\mathbf{H} = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k$ (since the working field here is $\mathbf{R}$, we will temporarily allow ourselves the use of the letter k for one of the generators of the space) where we have the relation $i^2 = j^2 = k^2 = ijk = -1$. If $a = x + yi + zj + wk$ then $\overline{a} = x - yi - zj - wk$ and the *norm* of a is $N(a) = a\overline{a} = x^2 + y^2 + z^2 + w^2$. We see from this that every nonzero element a has a multiplicative inverse, namely, $a^{-1} = \overline{a}/N(a)$ with $N(a^{-1}) = N(a)^{-1}$. Thus $\mathbf{H}^\times = \mathbf{H} \setminus \{0\}$. The *trace* of a is $(a + \overline{a})/2$.

Infinitesimals and the tangent space of the identity. Here we give a somewhat informal description of the tangent space of the identity element in a topological group. Let M be a topological group with identity element 1 that is also a subgroup of the multiplicative group of an algebra A. The tangent space T_1M at the point 1 is the space of all $a \in A$ such that $1 + \epsilon a$ is still in M, and here we encapsulate the fact that ϵ should be very small by letting ϵ be a nonzero formal parameter whose square is zero. The tangent space is closed under addition, since if a and b are elements of T_1M, then

$$(1 + \epsilon a)(1 + \epsilon b) = 1 + \epsilon a + \epsilon b + \epsilon^2 ab = 1 + \epsilon(a + b)$$

and we see that $a + b$ is also in the space. It is also clear that T_1M is closed under multiplication by scalars in the field, so that T_pM is a real vector space. The tangent space of a point $(p, q) \in M \times N$ is the product of spaces $T_pM \times T_qM$.

Let M and N be two such groups with identities 1_M and 1_N respectively and let $\phi : M \to N$ be a group homomorphism. We define the *differential* $d\phi$ to be the map from $T_{1_M}M$ to $T_{1_N}N$ such that the diagram

$$\begin{tikzcd}
T_{1_M}M \arrow[r, "d\phi"] \arrow[d, "\pi_N"] & T_{1_N}N \arrow[d, "\pi_N"] \\
M \arrow[r, "\phi"] & N
\end{tikzcd}$$

commutes, where $\pi_M(a) = 1_M + \epsilon a$ and $\pi_N(b) = 1_N + \epsilon b$. The commutativity of the above diagram tells us that $d\phi(a)$ is given by the formula $1_N + \epsilon d\phi(a) = \phi(1_M + \epsilon a)$ for $a \in T_{1_M}M$.

Tangent spaces are relevant because the inverse function theorem tells us that if $\phi : \mathbf{R}^n \to \mathbf{R}^n$ is a differentiable map and its derivative (Jacobian) at a point x is invertible, then there exists an open neighbourhood U of x that is homeomorphic to its image $\phi(U)$. If ϕ is also a group homomorphism, then we have the following lemma.

Lemma T. *Let $\phi : G \to H$ be a homomorphism of topological groups and suppose that there is an open neighbourhood $S \subseteq \phi(G)$ that contains the identity of H. If G is connected, then $\phi(G)$ is the connected component containing the identity in H.*

Proof. Since the function $h \mapsto h^{-1}$ is a continuous involution, S^{-1} is also open and so is $S \cap S^{-1}$, which still contains the identity. Thus we may assume without loss of generality that S is closed under inverses. Let $\langle S \rangle$ be the smallest subgroup of $\phi(G)$ with $S \subseteq \langle S \rangle$. It is easy to see that $\langle S \rangle = \bigcup_{h \in \langle S \rangle} hS$. For all $h \in \phi(G)$, left multiplication by h is a homeomorphism from $\phi(G)$ to itself, to $\langle S \rangle$ is open.

It remains to show that $\langle S \rangle$ is closed, so let $h \in \langle S \rangle^c$ be given. If $hs \in \langle S \rangle$ for some $s \in S$, then $h = hss^{-1} \in \langle S \rangle$. So hS is an open neighbourhood of h contained in $\langle S \rangle^c$, proving that $\langle S \rangle$ is indeed closed. Since $\langle S \rangle$ is nonempty, open, and closed in the connected group $\phi(G)$, $\langle S \rangle = \phi(G)$ and $\phi(G)$ is the connected component of the identity. ∎

Finally, we will take the following lemma on faith.

Lemma C. *If G is a Lie group with a connected compact Lie subgroup H such that G/H is also connected, then G is connected.* ∎

Exercise 2. *Describe $\mathrm{O}(V)$ and $\mathrm{SO}(V)$ when V is a nondegenerate quadratic space of dimension 4 over $\mathbf{R}$. How many connected components does the full orthogonal group have?*

Solution. (Marcel Goh and Jad Hamdan.) We will write $\mathrm{SO}(r,s)$ to denote $\mathrm{SO}(V)$ when V has signature (r,s), and write $\mathrm{SO}(n)$ for $\mathrm{SO}(n,0)$. The question has two largely unrelated parts. First we describe the components of the identity in the three separate cases. First we deal with the case $(r,s) = (4,0)$. Then

$$Q(x,y,z,w) = x^2 + y^2 + z^2 + w^2$$

and we can identify (V, Q) with $(\mathbf{H}, n)$. Note that the group $\mathbf{H}^\times \times \mathbf{H}^\times$ acts on V by setting $(g, h) * v = gvh^{-1}$. The norm of $(g, h) * v$ is $N(g)N(h^{-1})N(v)$, so for an element (g, h) to preserve the norm, it is necessary and sufficient that $N(g) = N(h)$. We can also assume that g and h have norm 1, since if $\lambda = N(g) = N(h)$, then $g = \lambda g'$ and $h = \lambda h'$ for some unit quaternions g' and h' and

$$(g, h) * v = (\lambda g', \lambda h') * v = \lambda g' v \lambda^{-1} h'^{-1} = g' v h'^{-1} = (g', h') * v.$$

In particular, if g and h are both real, then (g, h) sends any $v \in V$ to itself. Thus, letting $\mathbf{H}_1$ denote the set of quaternions with norm 1, we have the exact sequence

$$1 \longrightarrow \{(-1, -1), (1, 1)\} \longrightarrow \mathbf{H}_1 \times \mathbf{H}_1 \xrightarrow{\phi} \mathrm{O}(V).$$

Note that the last map ϕ in the sequence is not surjective. In fact, the image of ϕ is contained in SO(4), since if we represent the action of $(g, h) = (a_1 + a_2 i + a_3 j + a_4 k, b_1 + b_2 i + b_3 j + b_4 k)$ on a quaterion v as the action of a matrix on a vector in $\mathbf{R}^4$, then the matrix of the transformation is AB, where

$$A = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & b_4 & -b_3 \\ b_3 & -b_4 & b_1 & b_2 \\ b_4 & b_3 & -b_2 & b_1 \end{pmatrix}.$$

We have $AA^{\mathrm{T}} = I$ and $BB^{\mathrm{T}} = I$ so $(AB)(AB)^{\mathrm{T}} = I$, as prescribed for a member of $\mathrm{O}(V)$. But we also see that $\det(A) = N(g) = 1 = N(H) = \det(B)$, so that $\det(AB) = 1$ as well.

To show that $\mathrm{SO}(4) \subseteq \mathrm{im}(\phi)$, we need to find the tangent space of the identity in $\mathbf{H}_1$. if $1 + \epsilon(x + yi + zj + wk)$ has norm 1, then we must have

$$(1 + \epsilon x)^2 + \epsilon^2 y^2 + \epsilon^2 z^2 + \epsilon^2 w^2 = (1 + \epsilon x)^2 = 1,$$

so the trace x of the quaternion must be zero. Thus $T_1\mathbf{H}$ is 3-dimensional and $T_1(\mathbf{H}_1 \times \mathbf{H}_1)$ is 6-dimensional. On the other hand, the tangent space of the identity matrix I in SO(4) is the set of all matrices with $A^{\mathrm{T}} = -A$, since the condition that $(I + \epsilon A)(I + \epsilon A)^{\mathrm{T}}$ implies that $I + \epsilon(A + A^{\mathrm{T}}) = I$. This is a 6-dimensional space as well, since the diagonal of A must have all entries zero, and the rest of the matrix is determined by the choice of the six remaining entries in the upper triangle. Thus to show that $d\phi$ is invertible, it suffices to show it is injective.

Now for $(a, b) \in T_1(\mathbf{H}_1 \times \mathbf{H}_1)$, we note that $\phi(1 + \epsilon a, 1 + \epsilon b)$ is a map on $\mathbf{H}$ that sends v to $(1 + \epsilon a)v(1 + \epsilon b)^{-1}$. Since b has zero trace, $(1 + \epsilon b)^{-1} = 1 - \epsilon b$ and

$$\phi(1 + \epsilon a, 1 + \epsilon b)(v) = (1 + \epsilon a)v(1 + \epsilon b)^{-1} = (v + \epsilon av)(1 - \epsilon b) = v + \epsilon(av - vb).$$

Then since $\epsilon d\phi(a, b)$ equals $\phi(1 + \epsilon a, 1 + \epsilon b)$ minus the identity endomorphism, we have $d\phi(a, b)(v) = av - vb$. If $(a, b) \in \ker(d\phi)$, then $av - vb = 0$ for all $v \in \mathbf{H}$, and taking $v = 1$ in particular, we have $a = b$. Thus $av = va$ for all $v \in \mathbf{H}$ and we see that $a \in \mathbf{R}$. But we assumed that a has trace zero, so $(a, b) = (0, 0)$. We have shown that $d\phi$ is bijective, so by Lemma T, the image of ϕ is the connected component of the identity in O(4).

In the case $(r,s) = (3,1)$, we have $Q(x,y,z,w) = x^2 + y^2 + z^2 - w^2$ but we can perform a change of basis with $u = z+w$ and $v = z-w$ to get $Q(x,y,u,v) = x^2+y^2+uv$. Since $x^2+y^2 = (x+iy)(x-iy)$, we can identify (V,Q) with the set of all matrices

$$\left\{ \begin{pmatrix} x+iy & u \\ v & iy-x \end{pmatrix} : x,y,u,v \in \mathbf{R} \right\},$$

with the negative determinant as the norm. Letting $M^* = \det(M)M^{-1}$, we find that V is precisely the set of $M \in M_2(\mathbf{C})$ with $M^* = -\overline{M}$. We have $(AB)^* = B^*A^*$ for $A, B \in M_2(\mathbf{C})$, and this operation is also linear. The group $\mathrm{SL}_2(\mathbf{C})$ acts on V by $g * M = gM\overline{g}^{-1}$. Indeed,

$$(g*M)^* = (gM\overline{g}^{-1})^* = \overline{g}M^*g^* = -\overline{g}\overline{M}g^* = -\overline{gM\overline{g}^*} - \overline{g*M},$$

so $g * M$ is in V. Note that the center of $\mathrm{SL}_2(\mathbf{C})$ is $\{\pm I\}$, and we have the exact sequence

$$1 \longrightarrow \{\pm I\} \longrightarrow \mathrm{SL}_2(\mathbf{C}) \xrightarrow{\phi} \mathrm{O}(V).$$

Once again, the image of ϕ is connected. Now we find the tangent space of $\mathrm{SL}_2(\mathbf{C})$ at the identity. An element

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbf{C})$$

in this space satisfies $I + \epsilon A \in \mathrm{SL}_2(\mathbf{C})$, so $\det(I+\epsilon A) = 1 + \epsilon a + \epsilon d = 1$. This implies that $d = -a$. In other words, the trace of A is zero, and in particular we see that $A^* = -A$. Now we examine what $I + \epsilon A$ does to a matrix $M \in V$. We note first that

$$(I+\epsilon\overline{A})^{-1} = \begin{pmatrix} 1+\epsilon\overline{a} & \epsilon\overline{b} \\ \epsilon\overline{c} & 1-\epsilon\overline{a} \end{pmatrix}^{-1} = \begin{pmatrix} 1-\epsilon\overline{a} & -\epsilon\overline{b} \\ -\epsilon\overline{c} & 1+\epsilon\overline{a} \end{pmatrix} = I + \epsilon\overline{A^*}$$

So

$$(I+\epsilon A)M\overline{(I+\epsilon A)}^{-1} = (M+\epsilon AM)(I+\epsilon\overline{A^*}) = M+\epsilon AM+\epsilon M\overline{A^*} = M+\epsilon(AM-M\overline{A}),$$

telling us that $d\phi(A)$ takes matrices M to $AM - M\overline{A}$. We now investigate what it means for A to be in the kernel of $d\phi$. If $MA - M\overline{A}$ for all matrices M, then taking $M = I$, we see that $A = \overline{A}$, meaning that A has all real entries and $AM = MA$ for all M. This implies that A is a scalar multiple of the identity and since it has zero trace, A must be 0. We have found that $\ker(d\phi) = 0$, so the connected component of the identity is isomorphic to $\mathrm{SL}_2(\mathbf{C})/\{\pm I\}$.

The third case $(r,s) = (2,2)$ feels a bit like a combination of the two cases above. We have $Q(x,y,z,w) = x^2+y^2-z^2-w^2$ and with the substitutions $x = x+z, y = x-z, z = w+y, w = w-y$ (the variables on the left-hand side are not the same as the ones on the right-hand side), we have

$$Q(x,y,z,w) = xy - zw,$$

so we can identify (V,Q) with $(M_2(\mathbf{R}), \det)$. The group $\mathrm{GL}_2(\mathbf{R}) \times \mathrm{GL}_2(\mathbf{R})$ defines an action on $M_2(\mathbf{R})$ given by $(g,h) * M = gMh^{-1}$. For (g,h) to preserve the determinant we must have $\det g = \det h$. We can also require that g and h have determinant 1, because for any $\lambda \in \mathbf{R}$ we have $\det(\lambda g) = \det(\lambda h)$ and

$$\lambda g M (\lambda h)^{-1} = \lambda^2 g M \lambda^{-2} h^{-1} = g M h^{-1}.$$

Thus we have the exact sequence

$$1 \to \{(I, I), (-I, -I)\} \to \mathrm{SL}_2(\mathbf{R}) \times \mathrm{SL}_2(\mathbf{R}) \overset{\phi}{\to} \mathrm{O}(V).$$

The computation we performed above for the tangent space of $\mathrm{SL}_2(\mathbf{C})$ works when the entries are real as well, so we find that the tangent space of $\mathrm{SL}_2(\mathbf{R}) \times \mathrm{SL}_2(\mathbf{R})$ is the set of (A, B) such that $\operatorname{tr} A = \operatorname{tr} B = 0$. In particular, since the trace of B is zero, we can write

$$B = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

and the fact that $\det(I + \epsilon B) = 1$ implies that

$$(I + \epsilon B)^{-1} = \begin{pmatrix} 1 + a & b \\ c & 1 - a \end{pmatrix}^{-1} = \begin{pmatrix} 1 - a & -b \\ -c & 1 + a \end{pmatrix} = I - \epsilon B.$$

So

$$\phi(I+\epsilon A, I+\epsilon B)(M) = (I+\epsilon A)M(I+\epsilon B)^{-1} = (M+\epsilon AM)(I-\epsilon B) = M+\epsilon(AM-MB),$$

and $d\phi(A, B)(M) = AM - MB$. We argue as before to find that for $(A, B) \in \ker(d\phi)$, $A = B$ and A is a scalar of the identity with trace zero and thus $(A, B) = (0, 0)$. So $d\phi$ is injective and the image of ϕ is isomorphic to

$$\mathrm{SL}_2(\mathbf{R}) \times \mathrm{SL}_2(\mathbf{R}) / \{(I, I), (-I, -I)\}.$$

On to the second part of the question. The claim is that $\mathrm{O}(4)$ has two connected components and that $\mathrm{O}(3, 1)$ and $\mathrm{O}(2, 2)$ both have four. Since $\mathrm{SO}(V)$ is a subgroup of index 2 in the group $\mathrm{O}(V)$, it suffices to that $\mathrm{SO}(V)$ is connected in the definite case and that it has two connected components in the other two cases. We do this by induction, building up from smaller-dimensional instances.

Let V be a 4-dimensional quadratic space with signature (r, s). Note that $\mathrm{SO}(r, s)$ acts transitively on the set $X = \{x \in V : x \cdot x = 1\}$, which is the orbit of the point $e_1 = (1, 0, 0, 0)$. A matrix in $\mathrm{Stab}(e_1)$ has e_1 as its first row and column, so it must have the form

$$\begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix}$$

for some $M \in \mathrm{SO}(r-1, s)$. So by the orbit-stabiliser theorem, we have a diffeomorphism $\mathrm{SO}(r, s)/\mathrm{SO}(r - 1, s) \cong X$. We will proceed by induction.

The base cases are $\mathrm{SO}(1)$ and $\mathrm{SO}(1, 1)$; the former is $\{1\}$, which clearly has one connected component. On the other hand, $\mathrm{SO}(1, 1)$ consists of orthogonal 2×2 matrices $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $\det(M) = 1$ and

$$M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M^{\mathrm{T}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

This condition implies that $a = d$ and $b = c$, so we can write

$$\mathrm{SO}(1,1) = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R}) : a^2 - b^2 = 1; a, b \in \mathbf{R} \right\}$$

establishing a bijection from $\mathrm{SO}(1,1)$ to the algebraic set $x^2 - y^2 = 1$, a hyperbola with two branches on either side of the y-axis. This is in fact a homeomorphism, showing that $\mathrm{SO}(1,1)$ has two connected components.

In the definite case $(r,s) = (4,0)$ the induction is straightforward. The set X of elements of norm 1 in a quadratic space of signature $(n,0)$ is the unit sphere S^{n-1}, which is connected. Having shown that $\mathrm{SO}(1)$ is connected and that the quotient $\mathrm{SO}(n)/\mathrm{SO}(n-1) \cong S^{n-1}$ is connected for all $n > 1$, we apply Lemma C inductively to conclude that $\mathrm{SO}(n)$ is connected for all n.

For the indefinite cases, the induction is a bit more involved. The set of elements of unit norm in a quadratic space of signature $(1,2)$, $(1,3)$, or $(2,2)$ is the set of tuples (x,y,z) or (x,y,z,t) satisfying

$$x^2 - y^2 - z^2 = 1, \quad x^2 - y^2 - z^2 - t^2 = 1, \quad \text{or} \quad x^2 + y^2 - z^2 - t^2 = 1$$

respectively, where are all two-sheeted hyperboloids each with two connected components. In each case, let X^+ be the sheet containing $(0, \ldots, 1)$. If we let $\mathrm{SO}^+(r,s)$ be the set of matrices of $\mathrm{SO}(r,s)$ that preserve X^+, one can show that $\mathrm{SO}^+(r,s)$ is a subgroup of $\mathrm{SO}(r,s)$ with index 2. Using an orbit-stabiliser argument analogous to the one above, we find that $\mathrm{SO}^+(r,s)/\mathrm{SO}^+(r-1,s) \cong X^+$.

The set of unit elements in a space of signature $(1,1)$ is a hyperbola. We have also shown that $\mathrm{SO}(1,1)$ is homeomorphic to a hyperbola by explicit computation. Using this identification, we find that the set $\mathrm{SO}^+(1,1)$ is homeomorphic to a branch of $\mathrm{SO}(1,1)$ and is therefore connected. By repeated application of Lemma C and the fact that $\mathrm{SO}(r,s) \cong \mathrm{SO}(s,r)$ for all integers r, s, we conclude that $\mathrm{SO}^+(1,3)$ and $\mathrm{SO}^+(2,2)$ are connected. So $\mathrm{O}(1,3)$ and $\mathrm{O}(2,2)$ both have four connected components, and we already showed that $\mathrm{O}(4,0)$ has two, finishing the exercise. ▮

The Hilbert symbol. For this discussion, let k denote either $\mathbf{R}$ or $\mathbf{Q}_p$. For $a, b \in k^\times$, we define the *Hilbert symbol* (a,b) by setting

$$(a,b) = \begin{cases} 1, & \text{if } ax^2 + by^2 = z^2 \text{ has a nonzero solution } (x,y,z) \text{ in } k^3; \\ -1 & \text{otherwise.} \end{cases}$$

Note that $(a,b) = (a, c^2 b)$ for any element $c \in k^\times$, since the square can be absorbed into the variable. For $a, b \in k^\times$, further properties of the Hilbert symbol include

i) $(a,b) = (b,a)$ and $(a, b^2) = 1$;
ii) $(a,-a) = 1$ and $(a, 1-a) = 1$;
iii) if $(a,b) = 1$ then $(ac,b) = (c,b)$ for all $c \in k^\times$; and
iv) $(a,b) = (a,-ab) = \bigl(a,(1-a)b\bigr)$.

Furthermore, it can be shown that the Hilbert symbol is bilinear; that is, $(ac,b) = (a,b)(c,b)$ for all $a, b, c \in k^\times$.

Quadratic forms over $\mathbf{Q}_p$. Let (V, Q) be a quadratic space of rank n over $\mathbf{Q}_p$ and pick an orthogonal basis $(e_1, \ldots, e_n)$. Letting $a_i = e_i \cdot e_i$, we have $\operatorname{disc}(Q) = a_1 \cdots a_n$. The *Hasse-Witt invariant* of V is the product

$$\epsilon(V) = \prod_{i<j} (a_i, a_j);$$

we saw in class that this does not depend on the choice of orthogonal basis. We also saw that two quadratic forms over $\mathbf{Q}_p$ are equivalent (this means their respective matrices A and A' are related by $A' = BAB^{\mathrm{T}}$ for some invertible matrix B) if and only if they have the same rank, discriminant, and Hasse-Witt invariant.

Theorem Z. *Let (V, Q) be a quadratic space of rank n over $\mathbf{Q}_p$. Writing $d = \operatorname{disc}(Q) \in \mathbf{Q}_p/(\mathbf{Q}_p^\times)^2$ and letting $\epsilon = \epsilon(V)$ be the Hasse-Witt invariant of the space, there is a nonzero vector $x \in V$ with $Q(x) = x \cdot x = 0$ if and only if*

i) $n = 2$ and $d = -1$;

ii) $n = 3$ and $(-1, -d) = \epsilon$;

iii) $n = 4$ and either $d \neq 1$ or else $d = 1$ and $\epsilon = (-1, -1)$; or

iv) $n \geq 5$. ▮

Exercise 3. *Show that the Hilbert symbol (a, b) for $a, b \in \mathbf{Q}_p^\times$ is equal to -1 if and only if the idoneous central simple algebra over $\mathbf{Q}_p$ defined by*

$$B = \mathbf{Q}_p + \mathbf{Q}_p i + \mathbf{Q}_p j + \mathbf{Q}_p k,$$

where $i^2 = a$, $j^2 = b$, and $ij = -ji = k$, is a division algebra, and that it is isomorphic to the matrix algebra $\mathrm{M}_2(\mathbf{Q}_p)$ if $(a, b) = 1$.

Proof. (Sun Kai Leung and Paul-Antoine Seitz.) Call this central simple algebra A and let $q = x + yi + zj + wk \in A$. Defining $\overline{q} = x - yi - zj - wk$, a routine computation gives $q\overline{q} = x^2 - ay^2 - bz^2 + abw^2 \in \mathbf{Q}_p$. This is a quadratic form in the variables x, y, z, and w of discriminant $(ab)^2 \sim 1$. The Hasse-Witt invariant of the associated quadratic space is

$$\begin{aligned}
(1, -a)(1, -b)(1, ab)(-a, -b)(-a, ab)(-b, ab) &= (1, ab)(1, ab)(-a, -ab^2)(-b, ab) \\
&= (-a, -a)(-b, ab) \\
&= (-1, -a)(a, -a)(-b, b)(-b, a) \\
&= (-1, -1)(-1, a)(-b, a) \\
&= (-1, -1)(a, b).
\end{aligned}$$

If $(a, b) = -1$, by part (iii) of Theorem Z, we have $q\overline{q} \neq 0$ for all nonzero $q \in A$, so every $q \neq 0$ has an inverse $q^{-1} = \overline{q}/(q\overline{q})$. If $(a, b) = 1$, then there is some $(x, y, z, w) \neq (0, 0, 0, 0)$ such that $x^2 - ay^2 - bz^2 + abw^2 = 0$. Letting $q = x + yi + zj + wk$, we have $q \neq 0$ and $q\overline{q} = 0$, meaning that q is a zero divisor and thus A is not a division algebra. This settles the first part of the question.

In the case that $(a,b) = 1$, there is a nonzero vector $(x,y,z) \in \mathbf{Q}_p$ such that $z^2 = ax^2 + by^2$. We must have $z \neq 0$ and at most one of x and y is zero. Without loss of generality, suppose that $x \neq 0$. Defining

$$A = \frac{1}{x}\begin{pmatrix} z & -by \\ y & -z \end{pmatrix} \qquad \text{and} \qquad B = \frac{1}{x}\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix},$$

we have

$$A^2 = \frac{1}{x^2}\begin{pmatrix} z^2 - by^2 & -zby + zby \\ zy - zy & -by^2 + z^2 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI$$

and $B^2 = bI$, while

$$AB = \frac{1}{x}\begin{pmatrix} z & -by \\ y & z \end{pmatrix}\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} = \frac{1}{x}\begin{pmatrix} -by & bz \\ -z & by \end{pmatrix} = -\frac{1}{x}\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}\begin{pmatrix} z & -by \\ y & z \end{pmatrix} = -BA,$$

so that the map sending $i \mapsto A$, $j \mapsto B$, is an isomorphism of $\mathbf{Q}_p$-algebras between A and this matrix algebra. The proof concludes by noting that the span of $\{I, A, xB, xAB\}$ is all of $\mathrm{M}_2(\mathbf{Q}_p)$, since the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & b & 1 & 0 \\ z & -by & y & -z \\ -by & bz & -z & by \end{pmatrix}$$

has determinant $4b(by^2 - z^2) = -4ax^2b \neq 0$. In particular, the set $\{I, A, B, AB\}$ spans all of $\mathrm{M}_2(\mathbf{Q}_p)$ as well. ▮

Lemma Henselianum. *Ordo p-adicus* $v_p : \mathbf{Q}_p \to \mathbf{Z} \cup \{\infty\}$ est functio

$$v_p(x) = \begin{cases} n, & \text{si } x = p^n u, \text{ ubi } u \in (\mathbf{Z}/p\mathbf{Z})^\times; \\ \infty, & \text{si } x = 0. \end{cases}$$

Subanulus $\mathbf{Z}_p \subseteq \mathbf{Q}_p$ est copia elementorum $x \in \mathbf{Q}_p$ cum $v_p(x) \in \mathbf{N} \cup \{0, \infty\}$. *Norma p-adica* est $|x|_p = p^{-v_p(x)}$ et definimus spatiam metricum super $\mathbf{Q}_p$ cum functio distantiae $d_p(x,y) = |x-y|_p$. Sub illam functionem $\mathbf{Z}_p$ completum est; i.e., omnis sequentia Cauchiana limitem in spatio habet.

Polynomium $f(x_1, \ldots, x_m)$ cum coefficientibus in $\mathbf{Z}_p$ et solutionem aequatione $f(x_1, \ldots, x_m) \equiv 0 \pmod{p^n}$ dantur, et volumus levare hanc solutionem ad solutionem cum coefficientibus in $\mathbf{Z}_p$. Lemma sequens de polynomiis unae incognitae est.

Lemma G. *Sit f polynomium unae incognitae cum coefficientibus in $\mathbf{Z}_p$ et sit f' derivativum eius. Sit $x \in \mathbf{Z}_p$ cum $f(x) \equiv 0 \pmod{p^n}$ et $v_p\bigl(f'(x)\bigr) = k$, ubi n et k numeri integri sunt, et $0 \le 2k < n$. Tum existit $y \in \mathbf{Z}_p$ satisfaciens*

i) $f(y) \equiv 0 \pmod{p^{n+1}}$;

ii) $v_p\bigl(f'(y)\bigr) = k$; *et*

iii) $y \equiv x \pmod{p^{n-k}}$.

Demonstratio. Ponimus $y = x + p^{n-k}z$, ubi $z \in \mathbf{Z}_p$ eligetur postmodum. Hoc elementum y postulationem (iii) satisfacit. Ex formula Tayloriana sequitur

$$f(y) = f(x) = p^{n-k}zf'(x) + p^{2n-2k}z^2h(y),$$

ubi $h(y)$ elementum anuli $\mathbf{Z}_p$ est. Ex hypothesi $f(x) = p^n b$ cum $b \in \mathbf{Z}_p$ et $f'(x) = p^k c$ ubi $c \in \mathbf{Z}_p$ est elementum vertibile. Tum

$$f(y) = p^n(b + zc) + p^{2n-2k}z^2h(y)$$

scribere possumus, et eligentes z cum $b + zc \equiv 0 \pmod{p}$, habemus postulationem (i), quia $2n - 2k > n$. Ex formula Tayloriana cum f' habemus $f'(y) \equiv p^k c \pmod{p^{n-k}}$ et cum $n - k > k$, habemus propositionem (ii). ∎

Applicatio repetita huius lemmatis et completudo spatii lemma Henselianum producunt.

Theorema H. *Sit f polynomium m incognitarum cum coefficientibus in $\mathbf{Z}_p$. Sit $x = (x_1, \ldots, x_m) \in (\mathbf{Z}_p)^m$ ut $f(x) \equiv 0 \pmod{p^n}$ et $v_p\big(f_j(x)\big) = k$, ubi $1 \le j \le m$, k et n sunt numeri integri satisfacientes $0 \le 2k < n$, et f_j derivativum partiale functionis f est in incognita j^a. Tum existit $y \in (\mathbf{Z}_p)^m$ cum $f(y) = 0$ et satisfaciens $y \equiv x$ secundum modulum p^{n-k}.*

Demonstratio. Primo assumimus $m = 1$. Ex Lemmate G cum $x^{(0)} = x$ invenimus $x^{(1)} \in \mathbf{Z}_p$ ut $x^{(0)}$ et $x^{(1)}$ congrui sunt secundum modulum p^{n-k} et satisfaciens $f\big(x^{(1)}\big) \equiv 0 \pmod{p^{n+1}}$ et $v_p\big(f'(x^{(1)})\big) = k$. Tum applicamus Lemma G cum $x^{(1)}$. Sic inductiva mente construimus sequentiam $x^{(0)}, x^{(1)}, \ldots$ ubi indici generali q

$$x^{(q+1)} \equiv x^{(q)} \pmod{p^{n+q-k}} \qquad \text{et} \qquad f\big(x^{(q)}\big) \equiv 0 \pmod{p^{n+q}}$$

habemus. Haec sequentia Cauchiana est, quia omni integri $q, r > 0$ habemus $d_p\big(x^{(q+r)} - x^{(q)}\big) \le p^{-n-q+k}$. Tum sequentia verge ad limitem $y \in \mathbf{Z}_p$ satisfaciens $f(y) = 0$ et $y \equiv x \pmod{p^{n-k}}$.

Conditio indicis j casum generale ad casum $m = 1$ reducit. Consideramus polynomium $\tilde{f}$ unae incognitae cum formula

$$\tilde{f}(x) = f(x_1, \ldots, x_{j-1}, x, x_{j+1}, \ldots, x_m).$$

Deinde casum $m = 1$ propositionis applicare possumus cum $\tilde{f}$; ex illo invenimus $y_j \in \mathbf{Z}_p$ satisfaciens $y_j \equiv x_j \pmod{p^{n-k}}$ et $\tilde{f}(y_j) = 0$. Ponimus $y_i = x_i$ omni indici $i \ne j$ et elementum $y = (y_i)$ est solutio desiderata. ∎

Exercise 4. *Let p be an odd prime. Show that the quadratic form $ax^2 + by^2 + cz^2$ with coefficients in $\mathbf{Q}_p$, in which a, b, and c belong to $\mathbf{Z}_p^\times$, has a nontrivial zero, i.e., the associated quadratic space over $\mathbf{Q}_p$ is not anisotropic.*

Proof. (Davide Accadia and Niccolò Bosio.) First, we show that the equation $ax^2 + by^2 + cz^2 = 0$ has a nonzero solution in $\mathbf{Z}/p\mathbf{Z}$. We pick $z \in \mathbf{Z}/p\mathbf{Z}$ so that $c' = -cz^2 \neq 0$, reducing our problem to finding a solution (x, y) to the equation $ax^2 = c' - by^2$. Since a, b, and c are all nonzero in $\mathbf{Z}/p\mathbf{Z}$, there are $(p-1)/2+1$ elements in $\mathbf{Z}/p\mathbf{Z}$ of the form ax^2 and $(p-1)/2+1$ elements of the form $c' - by^2$, so these two sets must intersect in at least one element, giving us a nontrivial solution (x, y, z) to the equation.

It now remains to apply Theorem H to this solution (x, y, z) with $m = 3$, $n = 1$, and $k = 0$. (The gradient vector of f is $(2x, 2y, 2z)$, one of whose components must have p-adic valuation equal to 0 since $(x, y, z) \neq (0, 0, 0)$ and $p \neq 2$.) ∎

Integral lattices. We now turn to quadratic forms defined over the integers $\mathbf{Z}$. A *unimodular lattice* is a free abelian group of rank n with a symmetric bilinear form $x \cdot y$ such that

i) The homomorphism $L \to \mathrm{Hom}(L, \mathbf{Z})$ that sends $x \mapsto (y \mapsto x \cdot y)$ is an isomorphism.

ii) If (e_i) is a basis of L over $\mathbf{Z}$, then the determinant of the matrix $(e_i \cdot e_j)$ is ± 1.

The set $\mathrm{Hom}(L, \mathbf{Z})$, also denoted $L^\vee$, is called the *dual* of L, and the condition above explains why unimodular lattices are sometimes called self-dual. An element $x \in L$ can be identified with an element of $L^\vee$ if $x \cdot y$ is integer for all $y \in L$, and this is true for all x in a unimodular lattice. For any ring S admitting a homomorphism $\mathbf{Z} \to S$, we obtain an S-module $L \otimes S$ by extending the scalars from $\mathbf{Z}$ to S. Two lattices L_1 and L_2 are said to be *locally isomorphic* if $L_1 \otimes \mathbf{Z}_p \cong L_2 \otimes \mathbf{Z}_p$ for all primes p and $L_1 \otimes \mathbf{Z}_p \cong L_2 \otimes \mathbf{Z}_p$. The set of lattices that are locally isomorphic to a given lattice L is called the *genus* of L. We saw in class that two lattices in the same genus must have the same discriminant. Since $V = L \otimes \mathbf{R}$ is a quadratic space over $\mathbf{R}$, it has a well defined signature (r, s). As in the real case, we say that L is *positive definite* if $s = 0$, *negative definite* if $r = 0$, and *indefinite* otherwise. Given a quadratic module V, we will sometimes denote the corresponding quadratic space over a different ring R by V_R.

We say that a lattice L is *even* or *of type* II if the quadratic form associated to L takes only even values, and we say that L is *odd* or *of type* I otherwise. We saw in class that there is an element $u \in L$, unique modulo reduction modulo 2, such that $u \cdot x = x \cdot x \pmod 2$ for all $x \in L$. The image of $u \cdot u$ in $\mathbf{Z}/8\mathbf{Z}$ is an invariant of L, denoted $\sigma(L)$. If L is even, then $\sigma(L) = 0$.

Let $\langle 1 \rangle$ denote the 1-dimensional quadratic space with $Q(x) = x^2$ and let $\langle -1 \rangle$ denote the quadratic space with $Q(x) = -x^2$ (their bilinear forms are $x \cdot y = xy$ and $x \cdot y = -xy$ respectively). Note that unless r and s are both zero, the direct sum $\langle 1 \rangle^r \mathbin{\widehat{\oplus}} \langle -1 \rangle^s$ is an odd lattice. In class we saw the following structure theorem for indefinite unimodular lattices.

Theorem S. *Let L be a unimodular indefinite lattice of signature (r, s). If L is odd, then $L \cong \langle 1 \rangle^r \mathbin{\widehat{\oplus}} \langle -1 \rangle^s$. If L is even, then $r - s \equiv 0 \pmod 8$ and there is only one lattice in this case as well, up to isomorphism.* ∎

In the solution to the next exercise, we will also use the following lemma.

Lemma P. *Let L and L' be $\mathbf{Z}_p$-lattices of discriminant d with pairing matrices A and A' respectively. Let $\lambda = 1$ if p is odd and 3 if $p = 2$. If there exists $T \in \mathrm{M}_n(\mathbf{Z}_p)$ such that $T^{\mathrm{T}}AT = A' \pmod{p^\lambda}$, then there is X in $\mathrm{M}_n(\mathbf{Z}_p)$ such that $X^{\mathrm{T}}AX = A'$.* ▌

In most of the course, we have assumed that $p \neq 2$. But for the next exercise, the definition of a genus of a lattice requires that we consider $\mathbf{Z}_2$-lattices. We will thus require the following lemma, whose proof can be found in Serre (1973).

Lemma E. *An element $x \in \mathbf{Q}_2^\times$ is a square if and only if x can be written as $2^n u$ where n is even and $u \equiv 1 \pmod 8$.* ▌

Exercise 5. *Show that all even unimodular lattices of a given signature (r, s) are in the same genus. Show that all odd unimodular lattices are in the same genus. Give an example of two quadratic forms of the same discriminant that lie in different genera.*

Proof. (Martí Roset.) Theorem S allows us to consider only the definite case, and without loss of generality, we can further assume that both lattices are positive definite. Suppose that L_1 and L_2 are in the same genus. Then $L_1 \otimes \mathbf{Z}_2 \cong L_2 \otimes \mathbf{Z}_2$ and we find that $L_1 \otimes \mathbf{F}_2 \cong L_2 \otimes \mathbf{F}_2$. In these lattices over $\mathbf{F}_2$, either all vectors have zero length, in which case L_1 and L_2 were both even, or some vector has nonzero length, in which case both L_1 and L_2 were odd.

Now for the other direction of the proof, suppose that L_1 and L_2 are unimodular positive definite integral lattices. Since $L_i \mathbin{\widehat{\oplus}} \langle -1 \rangle$ is odd, unimodular, and indefinite, it is isomorphic to $L' = \langle 1 \rangle^n \mathbin{\widehat{\oplus}} \langle -1 \rangle$, which has $\operatorname{disc}(L') = -1$ and $\sigma(L') \equiv n - 1 \pmod 8$. The discriminant is multiplicative and the σ-invariant additive under orthogonal sum, so $\operatorname{disc}(L_i) = 1$ and $\sigma(L_i) \equiv n \pmod 8$. Furthermore, $L_1 \otimes \mathbf{R} \cong \langle 1 \rangle^n \cong L_2 \otimes \mathbf{R}$, so it remains to show that $L_1 \otimes \mathbf{Z}_p \cong L_2 \otimes \mathbf{Z}_p$ for all primes p.

When p is odd, we see that $L_1 \otimes \mathbf{F}_p$ and $L_2 \otimes \mathbf{F}_p$ have the same rank and discriminant, so by Lemma P we find that in fact $L_1 \otimes \mathbf{Z}_p \cong L_2 \otimes \mathbf{Z}_p$. In the case $p = 2$, we introduce some new notation. Let $\langle d \rangle$ denote the quadratic form of rank 1 given by $Q(x) = dx^2$. We will also abuse notation and denote a quadratic form by its pairing matrix. We then use the fact that any unimodular $\mathbf{Z}_2$-lattice is the orthogonal sum of copies of

$$\langle 1 \rangle, \quad \langle 3 \rangle, \quad \langle 5 \rangle, \quad \langle 7 \rangle, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

We have the relations

i) $\langle 1 \rangle^2 \cong \langle 5 \rangle^2$ and $\langle 3 \rangle^2 \cong \langle 7 \rangle^2$;

ii) $\langle 3 \rangle \mathbin{\widehat{\oplus}} \langle 5 \rangle \mathbin{\widehat{\oplus}} \langle 7 \rangle \cong \langle 1 \rangle \mathbin{\widehat{\oplus}} \langle 3 \rangle^2$;

iii) $\langle 1 \rangle^4 \cong \langle 7 \rangle^4$;

iv) $\langle d \rangle \mathbin{\widehat{\oplus}} A \cong \langle d \rangle \mathbin{\widehat{\oplus}} \langle 1 \rangle \mathbin{\widehat{\oplus}} \langle -1 \rangle$ for all $d \in \{1, 3, 5, 7\}$ and $A \in \{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)\}$; and

v) $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^2 \cong \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)^2$.

Now consider $L_i \otimes \mathbf{Z}_2$. Since L_i is even, it is an orthogonal sum of copies of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$, since any copies of $\langle d \rangle$ would cause the lattice to be odd. The discriminant of $L_i \otimes \mathbf{Z}_2$ is 1 and the discriminants of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ are -1 and 3 respectively, so we find that

$$L_i \otimes \mathbf{Z}_2 \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{r_1} \mathbin{\widehat{\oplus}} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}^{r_2}$$

with both r_1 and r_2 even, so by property (v) above we have $L_i \otimes \mathbf{Z}_2 \cong \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{r_1+r_2}$. If the L_i are odd, we have

$$L_i \otimes \mathbf{Z}_2 \cong \langle 1\rangle^{r_1} \mathbin{\widehat{\oplus}} \langle 3\rangle^{r_3} \mathbin{\widehat{\oplus}} \langle 5\rangle^{r_5} \mathbin{\widehat{\oplus}} \langle 7\rangle^{r_7}.$$

Since the discriminant is 1, either r_3, r_5, and r_7 are all even or they are all odd. If they are all odd, we the relation (ii) to make them all even (increasing r_1 in the process). Then we can use the relations in (i) to see that

$$L_i \otimes \mathbf{Z}_2 \cong \langle 1\rangle^{r_1} \mathbin{\widehat{\oplus}} \langle 7\rangle^{r_7},$$

for some r_1 and r_7 possibly different from above. Since L_i is positive definite of rank $r_1 + r_7$, $\sigma(L_i)$ must be congruent to $r_1 + r_7$ modulo 8, but on the other hand, from the right-hand side we must have $r_1 + r_7 \equiv r_1 + 7r_7 \pmod 8$. This means that r_7 is either 0 or 4 modulo 8, and we can use relation (iii) to find that $L_1 \otimes \mathbf{Z}_2 \cong \langle 1\rangle^n \cong L_2 \otimes \mathbf{Z}_2$.

To get lattices with the same discriminant lying in different genera, take an even lattice of discriminant 1, say the space E_8 we constructed in class, and an odd lattice of discriminant 1 of the same rank (we can take $\langle 1\rangle^8$ as the example corresponding to E_8). ▮

Modular forms and theta series. Let $\mathcal{H}$ denote the complex upper half-plane; that is, the set of $z \in \mathbf{C}$ with $\Im z > 0$. Given an lattice L of rank n, we define the *theta series* of L to be the sum

$$\theta_L(z) = \sum_{v\in L} e^{\pi i (v\cdot v) z},$$

where $z \in \mathcal{H}$. It is easy to see that $\theta_L(z+2) = \theta_L(z)$, and when L is unimodular, one can also show that

$$\theta_L\Big(\frac{-1}{z}\Big) = \Big(\frac{z}{i}\Big)^{n/2} \theta_L(z).$$

If L is even, then $v\cdot v$ is always even, so we actually have $\theta_L(z+1) = \theta_L(z)$, and we saw in class that the dimension n of an even unimodular lattice is always a multiple of 8, so the factor of $1/\sqrt{i}$ disappears and we have $\theta_L(-1/z) = z^{n/2}\theta_L(z)$. The significance of this becomes apparent when we note that the group $\mathrm{SL}_2(\mathbf{Z})$ of integral matrices with determinant 1 acts by Möbius transformations on the upper half-plane; for an element $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ and $z \in \mathcal{H}$, we have

$$g * z = \frac{az+b}{cz+d}.$$

Since the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generate $\mathrm{SL}_2(\mathbf{Z})$, the formulas above show that the theta series of an even unimodular lattice is invariant under the action of $\mathrm{SL}_2(\mathbf{Z})$, up to a factor of $z^{n/2}$.

A *modular form of weight k* on a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbf{Z})$ (which may be $\mathrm{SL}_2(\mathbf{Z})$ itself) is a holomorphic function $f : \mathcal{H} \to \mathbf{C}$ satisfying

$$f\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^k f(z)$$

and with an expansion

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z},$$

for some $a_n \in \mathbf{C}$. The space of all such functions is denoted $\mathcal{M}_k(\Gamma)$.

Exercise 6. *This exercise deals with odd unimodular lattices, which were largely left out of our discussion in class. In the following, $q = e^{2\pi i z}$ and $y = \Im z$.*

a) *Let L be an odd unimodular lattice of rank $2k$. Show that the theta series $\theta_L(z)$ is invariant under the group $\Gamma(2)$ consisting of matrices in $\mathrm{SL}_2(\mathbf{Z})$ that are congruent to the identity modulo 2.*

b) *To avoid having theta series with fractional powers of q, it is useful to redefine $\theta_L(q)$ by the rules*

$$\theta_L(z) = \sum_{v \in L} e^{2\pi i (v\cdot v) z} \qquad \text{and} \qquad \theta_L(q) = \sum_{v\in L} q^{v\cdot v} = \sum_{n=0}^{\infty} r_L(n) q^n,$$

where $r_L(n)$ denotes the number of vectors $v \in L$ with $v \cdot v = n$. Show that $\theta_L(q)$ is a modular form of weight k on the subgroup $\Gamma_0(4)$ consisting of matrices in $\mathrm{SL}_2(\mathbf{Z})$ that are upper triangular modulo 4.

c) *Although the Eisenstein series E_2 defined by*

$$E_2(q) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n,$$

where $\sigma_1(n) = \sum_{d\backslash n} d$, fails to be invariant under the action of $\mathrm{SL}_2(\mathbf{Z})$, the modification

$$E_2^*(z) = E_2(z) - \frac{3}{\pi y}$$

is a modular form of weight 2, though no longer holomorphic. Use this fact to show that the series

$$E_2^{(2)} = E_2(z) - 2E_2(2z) = E_2(q) - 2E_2(q^2)$$

and

$$E_2^{(4)} = E_2(z) - 4E_2(2z) = E_2(q) - 2E_2(q^4)$$

are (holomorphic) modular forms of weight 2 on $\Gamma_0(4)$.

d) *Show that any modular form of weight k on $\Gamma_0(4)$ has exactly $k/2$ zeroes on any fundamental region. Use this to conclude that $\mathcal{M}_2(\Gamma_0(4))$ is 2-dimensional, and thus spanned by the two Eisenstein series $E_2^{(2)}$ and $E_2^{(4)}$.*

e) Use the result of (d) to calculate the number of vectors of odd length in any odd unimodular quaternary quadratic form.

f) Write the theta series attached to the standard quaternary lattice $\mathbf{Z}^4$ with the standard dot product, and the theta series attached to the lattice

$$D_4 = \Bigl\{(a,b,c,d) \in \mathbf{Z}^4 \cup \Bigl(\mathbf{Z} + \frac{1}{2}\Bigr)^4 : a+b+c+d \in 2\mathbf{Z}\Bigr\}.$$

Deduce a closed form expression for the number of vectors of a given length in each of these two lattices.

Proof. For part (a), we first show that $\Gamma(2)$ is generated by the three matrices

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

To see this, note that for a general matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(2)$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b-2a \\ c & d-2c \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} a-2b & b \\ c-2d & d \end{pmatrix}.$$

Suppose that $b \ne 0$. Since $|a|$ is odd and $|b|$ is even, they are not equal. if $|a|$ is larger, we use the division algorithm to find q, r such that $|a| = |2b|q + r$, where $|r| < |b|$, and then apply the second transformation q times to strictly reduce the absolute value of the top-left matrix entry. If $|b|$ is larger, we reduce the absolute value of the top-right entry in a similar fashion. We can keep doing this until $b = 0$, in which case the matrix must be some integer power of $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$, after possibly multiplying by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Thus it suffices to prove invariance under the three generators of $\Gamma(2)$. The negative identity matrix acts as the identity Möbius transformation, and we already saw that theta series are invariant under the transformation $z \mapsto z+2$. The last generator is $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$, which also poses no problem, since

$$\theta_L\Bigl(\frac{z}{2z+1}\Bigr) = \Bigl(\frac{i}{z}\Bigr)^k \theta_L\Bigl(\frac{-2z-1}{z}\Bigr) = \Bigl(\frac{i}{z}\Bigr)^k \theta_L\Bigl(\frac{-1}{z}\Bigr) = \Bigl(\frac{i}{z}\Bigr)^k \Bigl(\frac{z}{i}\Bigr)^k \theta_L(z) = \theta_L(z).$$

We start part (b) by claiming that $\Gamma(2)$ and $\Gamma_0(4)$ are conjugate in $\mathrm{SL}_2(\mathbf{Q})$, by the element $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Indeed, for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a/2 & b/2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b/2 \\ 2c & d \end{pmatrix},$$

and if $\gamma \in \Gamma(2)$ to begin with, then $2c$ is a multiple of 4 so the result is in $\Gamma_0(4)$. On the other hand,

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c/2 & d \end{pmatrix}.$$

In this case, if $\gamma \in \Gamma_0(4)$, then bc is even so a and d must be odd for $ad - bc$ to equal 1. Since c was a multiple of 4, we have $c/2$ even and of course, so is $2b$, so the result is in $\Gamma(2)$. This gives a set of generators for $\Gamma_0(4)$; since

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix},$$

the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

comprise a set of generators for $\Gamma_0(4)$.

We shall call the modified theta series in part (b) $\theta'_L(z)$, to know when we have an extra factor of two and when we do not. Invariance under $z \mapsto z + 1$ is easy, since

$$\theta'_L(z+1) = \theta_L(2z+2) = \theta_L(2z) = \theta'_L(z).$$

For the other nontrivial transformation, we first note that

$$\theta'_L\left(\frac{-1}{4z}\right) = \theta_L\left(\frac{-1}{2z}\right) = \left(\frac{2z}{i}\right)^k \theta_L(2z) = \left(\frac{2z}{i}\right)^k \theta'_L(z).$$

We now have all we need to show that $\theta'_L(z)$ is a modular form of weight k on $\Gamma_0(4)$, because for the Möbius transformation $z \mapsto z/(4z+1)$ we have

$$\begin{aligned} \theta'_L\left(\frac{z}{4z+1}\right) &= \theta'_L\left(\frac{-1}{4(-1/(4z)-1)}\right) \\ &= \left(2i\left(\frac{1}{4z}+1\right)\right)^k \theta'_L\left(\frac{-1}{4z}-1\right) \\ &= \left(2i\left(\frac{1}{4z}+1\right)\right)^k \theta'_L\left(\frac{-1}{4z}\right) \\ &= \left(2i\left(\frac{2z}{i}\right)\left(\frac{1}{4z}+1\right)\right)^k \theta'_L(z) \\ &= (4z+1)^k \theta'_L(z). \end{aligned}$$

For part (c), we begin by noting that since

$$E_2(z) - NE_2(Nz) = E_2(z) - \frac{3}{\pi y} - NE_2(Nz) - N\frac{3}{N\pi y} = E_2^*(z) - NE_2^*(Nz),$$

for any $N \geq 2$, in particular both $E_2^{(2)}$ and $E_2^{(4)}$ are holomorphic and we are done if we can show that $E_2^*(2z)$ and $E_2^*(4z)$ are modular forms of weight 2 on $\Gamma_0(4)$. In fact, for all $N \geq 2$ we shall show that if $g(z)$ is a modular form of weight 2 on $\mathrm{SL}_2(\mathbf{Z})$, then

$f(z) = g(Nz)$ is a modular form of weight k on $\Gamma_0(N)$. (This would settle the question since $\Gamma_0(4) \subseteq \Gamma_0(2)$ and any modular form on $\Gamma_0(2)$ is automatically a modular form on $\Gamma_0(4)$.) Well, letting $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, we have

$$f\Bigl(\frac{az+b}{cz+d}\Bigr) = g\Bigl(N\frac{az+b}{cz+d}\Bigr) = g\Bigl(\frac{Naz+Nb}{cz+d}\Bigr) = g\Bigl(\frac{a(Nz)+Nb}{(c/N)(Nz)+d}\Bigr).$$

But since c is a multiple of N, the matrix $\left(\begin{smallmatrix} a & Nb \\ c/N & d \end{smallmatrix}\right)$ has integral entries and has determinant $ad - (Nb)(c/N) = ad - bc = 1$. So g is weight-2 invariant under its action, and

$$f\Bigl(\frac{az+b}{cz+d}\Bigr) = g\Bigl(\frac{a(Nz)+Nb}{(c/N)(Nz)+d}\Bigr) = \bigl((c/N)(Nz)+d\bigr)^2 g(Nz) = (cz+d)^2 f(z).$$

To begin part (d), we first show that $\Gamma_0(4)$ is a subgroup of index 6. We already found that $\Gamma(2)$ and $\Gamma_0(4)$ are conjugate subgroups of $\mathrm{SL}_2(\mathbf{Q})$, which means they have the same index in $\mathrm{SL}_2(\mathbf{Z})$. Furthermore, we a homomorphism from $\mathrm{SL}_2(\mathbf{Z})$ to $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$ given by reduction of entries modulo 2, giving the short exact sequence

$$1 \longrightarrow \Gamma(2) \longrightarrow \mathrm{SL}_2(\mathbf{Z}) \longrightarrow \mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z}) \longrightarrow 1.$$

An element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$ must have $ad - bc = 1$ in $\mathbf{Z}/2\mathbf{Z}$, so either $ad = 1$ and $bc = 0$ or vice versa. In each case there are three ways to make a product equal to 0, so the cardinality of $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$ is 6. We saw in class that any fundamental domain of the action of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half-plane has $k/12$ zeroes of a modular form (counting fractional zeroes on the boundary). So let F be a modular form of weight 12 on $\mathrm{SL}_2(\mathbf{Z})$ with its single zero at, say, $2i$ (chosen because it is right in the middle of the usual fundamental domain for $\mathrm{SL}_2(\mathbf{Z})\backslash\mathcal{H}$). Since $\Gamma_0(4)$ is an index-6 subgroup of $\mathrm{SL}_2(\mathbf{Z})$, we know that F has 6 zeroes on $\Gamma_0(4)\backslash\mathcal{H}$ and F^k has $6k$ zeroes on the same region. Now let $g \in \mathcal{M}_2\bigl(\Gamma_0(4)\bigr)$ be given, with m zeroes on $\Gamma_0(4)\backslash\mathcal{H}$. We want to show that $m = k/2$. Well, whatever m is, we know that g^{12} has $12m$ zeroes. Now we consider the function g^{12}/F^k, which is meromorphic on the compact Riemann surface $\Gamma_0(4)\backslash\mathcal{H}$ and thus has as many zeroes as poles. The number of zeroes it has is $12m$ and the number of poles it has is $6k$. So $m = k/2$, which is what we wanted to show.

In particular, any modular form of weight 2 on $\Gamma_0(4)$ has exactly one zero. Evaluating $E_2(q)$ at $q = 0$ (equivalent to evaluating $E_2(z)$ at $z = i\infty$) gives a value of 1, so $E_2^{(2)}(0) = -1$ and $E_2^{(4)}(0) = -3$. From here we see that $F(z) = 3E_2^{(2)}(z) - E_2^{(4)}(z)$ has a zero at $i\infty$, meaning that it has no zeroes on the upper half-plane $\mathcal{H}$. So, given any modular form f on $\Gamma_0(4)$ of weight 2, we can subtract a multiple of $E_2^{(2)}$ to get a form that has a zero at $i\infty$, and then divide by F to get a modular form of weight 0, which must be a constant. Symbolically, this amounts to showing that any f satisfies

$$\frac{f - \lambda E_2^{(2)}}{F} = \mu$$

for some $\lambda, \mu \in \mathbf{C}$; that is, $f = \lambda E_2^{(2)} + \mu F$. Since $E_2^{(2)}$ and $E_2^{(4)}$ are linearly independent, we have shown that $\mathcal{M}_2\bigl(\Gamma_0(4)\bigr)$ is 2-dimensional, bringing us to the end of part (d).

For part (e), we have the general formula

$$\sigma_1(n/N) - N\sigma_1(n/N) = \sum_{d\backslash n} d - \sum_{d\backslash(n/N)} Nd = \sum_{d\backslash n} d - \sum_{N\backslash d\backslash n} d = \sum_{N\not\backslash d\backslash n} d.$$

We saw that for any lattice L of rank $2k$, $\theta_L'(q)$ is a modular form of weight k on $\Gamma_0(4)$, so by the result of the previous section, we can write $\theta_L' = \lambda E_2^{(2)} + \mu E_2^{(4)}$ and by equating coefficients, we find that the number of vectors of length $n \geq 1$ in L is

$$r_L(n) = \lambda \sum_{2\not\backslash d\backslash n} d + \mu \sum_{4\not\backslash d\backslash n} d.$$

We can determine λ and μ from $r_L(0)$ and $r_L(1)$. Since the constant terms of $E_2^{(2)}$ and $E_2^{(4)}$ are -1 and -3 respectively, we have $r_L(0) = -\lambda - 3\mu$. So we have the simultaneous equations

$$\begin{pmatrix} r_L(0) \\ r_L(1) \end{pmatrix} = \begin{pmatrix} -1 & -3 \\ -24 & -24 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix},$$

which we can solve to get

$$\lambda = \frac{r_L(0)}{2} - \frac{r_L(1)}{16} \qquad \text{and} \qquad \mu = \frac{r_L(1)}{48} - \frac{r_L(0)}{2}.$$

Finally, we have come to part (f). We start by noting that both of these lattices have exactly one vector of length 0. There are 8 ways to make a vector of length 1 in $\mathbf{Z}^4$, since there are four slots to put either a 1 or -1. There are also 8 ways to make a vector of length 1 in D_4, since the 16 vectors of the form $(\pm 1/2, \pm 1/2, \pm 1/2, \pm 1/2)$ have norm 1, but only half of them have an even number of $-1/2$s, which is necesssary for the sum of the coordinates to be even. Invoking part (e) now, we find that $\lambda = 0$ and $\mu = -1/3$. Hence both lattices have theta series $-E_2^{(4)}/3$. ∎

Exercise 7. *Let G be a group acting transitvely on a set X. Let $x_0 \in X$ and let S be a subset of G such that for all $x \in X$, there exists $g \in S$ with $gx_0 = x$. Show that G is generated by S together with the stabiliser of x_0.*

Proof. Let $g \in G$. There exists $x \in X$ (namely, $g^{-1}x$) such that $gx = x_0$. Now by the property of S, there is $s \in S$ with $sx_0 = x$. So we see that $gsx_0 = x_0$, meaning that $gs \in \mathrm{Stab}(x_0)$. But this means that $g = gs \cdot s^{-1}$, and since G is closed under inverses, $G = G^{-1} = \left(\mathrm{Stab}(x_0)S^{-1}\right)^{-1} = S\,\mathrm{Stab}(x_0)$. ∎

The projective line. For the next exercise, we define the *projective line* $\mathbf{P}^1(k)$ over a field k to be the set $k^2 \setminus \{(0,0)\}$ quotiented by the equivalence relation $\sim$ that deems $(x, y) \sim (\lambda x, \lambda y)$ for any nonzero scalar $\lambda \in k$. We denote the equivalence class of (x, y) by $[x : y]$. If $y \neq 0$, we see that $[x : y] = [z : 1]$ for some $z \in k$. The element $[1 : 0]$ is the only element that cannot be written in this way; it is called *the point at infinity.*

Exercise 8. *Let k be a field. Show that* $\mathrm{SL}_2(k)$ *is generated by matrices of the form*

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \qquad \textit{and} \qquad \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

for $t \in K$ and $a \in K^\times$, along with $w = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. More precisely, show that $\mathrm{SL}_2(k) = B \sqcup BwB$, *where B is the subgroup of upper triangular matrices. This is known as the Bruhat decomposition of* $\mathrm{SL}_2(k)$.

Proof. The group $\mathrm{SL}_2(k)$ acts on the set $\mathbf{P}^1(k)$ by matrix multiplication; that is,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} [x : y] = [ax + by : cz + dy].$$

To see that this action is transitive, note that $\mathrm{GL}_2(k)$ is transitive on the set of nonzero vectors in k^2, and scaling the matrix to insist that it has determinant 1, we do not change its output in the projective line. Note that

$$Bw[1:0] = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : a, b, d \in k \right\} = \bigl\{ [-b : -d] : b, d \in k \bigr\}.$$

Since $ad = 1$, d cannot be zero, and we can divide out by $-d$ to find that this is the set $\bigl\{[z : 1] : z \in k\bigr\}$. In particular, the identity matrix I is not a member of Bw, but for any $p \in \mathbf{P}^1(k)$, there exists $\gamma \in S = Bw \sqcup \{I\}$ such that $\gamma[1 : 0] = p$. Note also that any upper triangular matrix fixes the point $[1 : 0]$, and if any $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ fixes $[1 : 0]$, then its bottom-left entry must be zero, so $\mathrm{Stab}([1 : 0]) = B$. Applying the result of Exercise 7 with $x_0 = [1 : 0]$ gives us

$$\mathrm{SL}_2(k) = S \cdot \mathrm{Stab}([1:0]) = (Bw \sqcup \{I\})B = BwB \sqcup B,$$

which is what we wanted. ∎

Exercise 9. *Show that every element of* $\mathrm{SL}_2(\mathbf{R})$ *can be written uniquely in the form*

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{1/2} & 0 \\ 0 & y^{-1/2} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

for $x \in \mathbf{R}$, $y \in \mathbf{R}^{>0}$, and $\theta \in [0, 2\pi)$. This is known as the Iwasawa decomposition of $\mathrm{SL}_2(\mathbf{R})$.

Proof. The set $\mathrm{SL}_2(\mathbf{R})$ acts on the upper half-plane $\mathcal{H}$ by Möbius transformations. We let

$$S = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{1/2} & 0 \\ 0 & y^{-1/2} \end{pmatrix} : x \in \mathbf{R},\ y > 0 \right\},$$

and note that

$$\begin{pmatrix} y^{1/2} & xy^{1/2} \\ 0 & y^{-1/2} \end{pmatrix} * i = \frac{y^{1/2} i + xy^{1/2}}{y^{-1/2}} = x + iy,$$

so since $x \in \mathbf{R}$ and $y > 0$ we see that for any $z \in \mathcal{H}$, there is some element of S such that $S * i = z$. Now the stabiliser of i is the set of all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbf{R})$ with

$$\frac{ai+b}{ci+d} = i.$$

This equation implies that $a = d$ and $b = -c$, which, along with the condition $ad - bc = 1$, gives $a^2 + b^2 = 1$ and we see that the set of all such matrices can be parametrised by letting $a = \cos\theta$ and $b = \sin\theta$. We are now in the fortunate position to apply Exercise 7 once again.

We have shown that for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$, there are x, y, and θ such that

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{1/2} & 0 \\ 0 & y^{-1/2} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(For convenience, we construct γ^{-1} instead of γ.) Given only the triple (x, y, θ), we can work backwards to find the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ above. Since the bottom-left entry on the right-hand side is zero, we have $c\cos\theta = a\sin\theta$, whence $c = a\tan\theta$. In the next multiplication, we find that $ya^2 + yc^2 = 1$, so

$$a = \frac{1}{\sqrt{y(1+\tan\theta)}} \qquad \text{and} \qquad c = \frac{\tan\theta}{\sqrt{y(1+\tan\theta)}}.$$

Lastly, from the equations $ab + cd = -x(a^2 + c^2)$ and $ad - bc = 1$, we find that

$$b = \frac{c - ax(a^2+c^2)}{a^2+c} \qquad \text{and} \qquad d = \frac{1+bc}{a},$$

finishing the proof of uniqueness. ▮

The Fourier transform. Let f be a Schwartz function on a finite-dimensional vector space V over $\mathbf{R}$. (We will not concern ourselves with exactly what a Schwartz function is; one should think of it as having nice decay properties at infinity.) The *Fourier transform* $\widehat{f}$ of f is the integral

$$\widehat{f}(y) = \int_V f(x) e^{-2\pi i (x\cdot y)}\, dx.$$

The Fourier transform over other quadratic spaces is given similarly, though in these settings we have to change what we mean by "nice" function. On $\mathbf{Q}_p$, we can take compactly supported functions. Of course, when we integrate over $\mathbf{Q}_p$, we'll need to know what measure we are integrating against. Luckily, there is a translation-invariant, countably additive measure μ on $\mathbf{Q}_p$ called the *Haar measure*, which we shall use without worrying about the details of its construction. Now that we have a measure (Lebesgue or Haar) on V, we can define the *covolume* of L as the measure of a fundamental region of V/L.

Additive characters. An *additive character* is a homomorphism from an abelian group Z to the unit circle; that is, for $x, y \in Z$ we have $\chi(x+y) = \chi(x)\chi(y)$. A character is said to be *trivial* if it assigns the value 1 to every member of the group. The following lemma is a simple consequence of definitions, but is extremely useful.

Lemma Z. *Let χ be a nontrivial character on an additive group Z. Then*

$$\sum_{x\in G}\chi(x)=0.$$

Proof. Since χ is nontrivial, there must be some $x_0\in Z$ with $\chi(x)\neq 1$. Then writing

$$\sum_{x\in G}\chi(x)=\sum_{x\in G}\chi(x_0+x)=\chi(x_0)\sum_{x\in G}\chi(x),$$

we see that this sum must be zero. ▮

Before proceeding, we stop to prove a miscellaneous lemma about containment of $\mathbf{Z}_p$-lattices. It will be useful in a couple of the exercises below.

Lemma B. *Let L and L' be $\mathbf{Z}_p$-lattices of the same rank. There exists a positive integer m such that $p^mL\subseteq L'$.*

Proof. Being free abelian groups, L and L' both have $\mathbf{Z}_p$-bases; call the matrices with these bases as columns B and B' respectively. These bases are also $\mathbf{Q}_p$-bases for the associated quadratic space $V_{\mathbf{Q}_p}$. The matrix X such that $B=XB'$ has finitely many entries, all of which are p-adic rationals. Thus there is an m for which p^mX has entries in $\mathbf{Z}_p$. Now given a vector $v=p^mw\in p^mL$, we can express it as a linear combination of vectors in B' by multiplying it by X on the left. Since p^mX and w both have entries consisting entirely of p-adic integers, $Xv=Xp^mw=(p^mX)w$ also consists entirely of p-adic integers. Hence we can express v as a $\mathbf{Z}_p$-linear combination of vectors in L'. ▮

Exercise 10. *Show that the characteristic function on $\mathbf{Z}_p$ is equal to its Fourier transform. More generally, let V be a quadratic space over $\mathbf{Q}_p$ and let L be a $\mathbf{Z}_p$-sublattice of V. Show that the Fourier transform of L is $\mu(L)$ times the characteristic function of the $\mathbf{Z}_p$-dual lattice; that is,*

$$\widehat{\mathbf{1}_L}=\mu(L)\mathbf{1}_{L^\vee}.$$

Proof. Expanding the definition of the Fourier transform gives

$$\widehat{\mathbf{1}_L}(x)=\int_V \mathbf{1}_L(y)e^{-2\pi i(x\cdot y)}\,dy=\int_L e^{-2\pi i(x\cdot y)}\,dy.$$

If x is an element of the dual, then $x\cdot y$ is an integer for all $y\in L$, so the integrand is 1 and the integral equals $\mu(L)$. If not, then $\chi(y)=e^{-2\pi i(x\cdot y)}$ is a nontrivial character. The kernel of χ is a sublattice of L, so by Lemma B, there is n such that $\ker\chi\supseteq p^nL$, so by translation-invariance of the measure μ,

$$\begin{aligned}\int_L e^{-2\pi i(x\cdot y)}\,dy &= \sum_{v\in L/p^nL}\int_{v+p^nL}\chi(y)\,dy\\ &= \sum_{v\in L/p^nL}\chi(v)\int_{p^nL}\chi(y)\,dy\\ &= \sum_{v\in L/p^nL}\chi(v)\int_{p^nL}1\,dy\\ &= \mu(p^nL)\sum_{v\in L/p^nL}\chi(v).\end{aligned}$$

But this is zero because the sum of a nontrivial character over a group is zero, by Lemma Z. ▮

Adèles. We let

$$\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p,$$

where the product is taken over all primes p. We then define $\mathbf{A}_{\mathbf{Z}} = \mathbf{R}\times\widehat{\mathbf{Z}}$. The *ring of adèles* $\mathbf{A}_{\mathbf{Q}}$ is the tensor product $\mathbf{A}_{\mathbf{Q}} = \mathbf{Q}\otimes_{\mathbf{Z}}\mathbf{A}_{\mathbf{Z}}$. An element in this ring is an infinite tuple consisting of a real number and one p-adic rational for each p, all but finitely many of which are p-adic integers.

Exercise 11. *Let L be a lattice of covolume 1 in a quadratic space V. The Poisson summation formula on $V_{\mathbf{R}}$ asserts that*

$$\sum_{v\in L}\phi(v) = \sum_{v\in L^\vee}\widehat{\phi}(v),$$

for all Schwartz functions ϕ on $V_{\mathbf{R}}$, where $L^\vee$ is the dual lattice of V. The adèlic Poisson summation formula asserts that

$$\sum_{v\in V}\phi(v) = \sum_{v\in V}\widehat{\phi}(v),$$

for all adèlic Schwartz functions ϕ on $V_{\mathbf{A}_{\mathbf{Q}}}$. Show that the adèlic Poisson summation formula implies its more familiar analogue on $V_{\mathbf{R}}$.

Proof. Given a Schwartz function ϕ on $\mathbf{R}$, we take our Schwartz function on the adèle ring to be $f = \phi\otimes\mathbf{1}_{L\otimes\widehat{\mathbf{Z}}}$. We have

$$\sum_{v\in L}\phi(v) = \sum_{v\in V}\mathbf{1}_{L\otimes\widehat{\mathbf{Z}}}(v)\phi(v) = \sum_{v\in V}f(v).$$

By the adèlic Poisson summation formula, the right-hand side becomes

$$\sum_{v\in V}f(v) = \sum_{v\in V}\widehat{f}(v),$$

but by the previous exercise, the Fourier transforms at the p-adic components are characteristic functions of dual lattices. So

$$\sum_{v\in V}\widehat{f}(v)=\sum_{v\in V}\mathbf{1}_{L^\vee\otimes\widehat{\mathbf{Z}}}\widehat{\phi}(v)=\sum_{v\in L^\vee}\widehat{\phi}(v),$$

which is what we were aiming to show. ∎

Exercise 12. *Let $G=\mathrm{GL}_n(\mathbf{Q}_p)$ and let $X=\mathrm{GL}_n(\mathbf{Q}_p)/\mathrm{GL}_n(\mathbf{Z}_p)$. Show that the action of G on X satisfies the finiteness assumption that was made in class when we discussed Hecke operators, i.e., that the stabiliser of any $x\in X$ acts on X with finite orbits.*

Proof. We want to show that for all $x\in X$, the set $\mathrm{Stab}_G(x)y$ is finite. Note that $\mathrm{Stab}_G(e)=\mathrm{GL}_n(\mathbf{Z}_p)$, and for general $x\in X$, we have

$$\mathrm{Stab}_G(x)=x\,\mathrm{GL}_n(\mathbf{Z})x^{-1}.$$

So for $y\in X$, $\mathrm{Stab}(x)y=x\,\mathrm{GL}_n(\mathbf{Z}_p)x^{-1}y$ and we are done if we can show that $\mathrm{GL}_n(\mathbf{Z}_p)z$ is finite for any $z\in X$. By applying Lemma B with $L=z\mathbf{Z}_p^n$ and $L'=\mathbf{Z}_p^n$, we obtain m such that $zp^m\mathbf{Z}_p^n\subseteq\mathbf{Z}_p^n$. Then we apply Lemma B again with $L=\mathbf{Z}_p^n$ and $L'=zp^m\mathbf{Z}_p^n$ to get $k\geq m$ such that $p^k\mathbf{Z}_p^n\subseteq p^mz\mathbf{Z}_p^n$.

Now letting $L=p^m\mathbf{Z}_p^n$, we can associate to any $x\in X$ the sublattice xL of $\mathbf{Q}_p^n$. If x and x' are different, then these sublattices are different, so our problem reduces to showing that the set of lattices of the form γzL, where $\gamma\in\mathrm{Stab}_G(x)$, is finite. Since γ comes from a conjugate of $\mathrm{GL}_n(\mathbf{Z}_p)$, it fixes $\mathbf{Z}_p^n$, so have the chain of inclusions

$$p^k\mathbf{Z}_p^n\subseteq\gamma(zL)\subseteq\mathbf{Z}_p^n,$$

showing that any such lattice of the prescribed form is a subgroup of $\mathbf{Z}_p^n$ containing $p^k\mathbf{Z}_p^n$. By the correspondence theorem, these subgroups are in bijection with elements of

$$\mathbf{Z}_p^n/(p^k\mathbf{Z}_p^n)\cong(\mathbf{Z}/p^k\mathbf{Z})^n,$$

which is finite. ∎

Exercise 13. *Let L be a unimodular $\mathbf{Z}_p$-lattice in a quadratic space V over $\mathbf{Q}_p$, and let G be the orthogonal group over $\mathbf{Z}_p$ attached to L. Show that $G(\mathbf{Q}_p)$ acts transitively on the set of pairs (L_1,L_2) of unimodular lattices satisfying $L_1/(L_1\cap L_2)\cong\mathbf{Z}/p\mathbf{Z}$.*

Proof. (Reginald Lybbert.) We write $L\sim_p L'$ if $L/(L\cap L')\cong\mathbf{Z}/p\mathbf{Z}$ and we take it as a fact (it was shown in class) that this is a symmetric relation. We shall also assume that $p\neq2$, for the sake of everyone's sanity. Since $G(\mathbf{Q}_p)$ acts transitively on lattices, we can assume that the first lattice in each tuple is the same. It is then enough to show that for any (L,L_1) and (L,L_2), we can find a map stabilising L that sends L_1 to L_2. (We will allow ourselves the use of L for a general unimodular lattice, not necessarily the one in the definition of G.) Note first that $pL_1\subseteq L$, since it is contained in the kernel of $L_1\to\mathbf{Z}/p\mathbf{Z}$, which is $L_1\cap L$. The kernel of $L\to L/pL$ is of course pL, so the kernel of $\phi:pL_1\to L/pL$ is $pL1\cap pL$. So we have

$$\phi(pL_1)\cong\frac{pL_1}{pL_1\cap pL}\cong\frac{L_1}{L_1\cap L}\cong\frac{\mathbf{Z}}{p\mathbf{Z}}.$$

This is some line in L/pL, and it is isotropic because the length of any element in L_1 is integer. Multiplying by p, the length of the element in L/pL is a multiple of p and thus 0. In fact, there is a correspondence between p-neighbours of L and isotropic lines in L/pL. Given an isotropic line in L/pL, we see that it's preimage must lie in $L \cap L'$ for some lattices L and L'. But we know what L is, so we can deduce the lattice L' for which the isotropic line is $\phi(pL')$. This shows the relation is one-to-one.

To show that the relation is surjective, we take an isotropic line in L/pL, spanned by an element $\overline{v} \in L$; by Hensel's lemma (since $p \neq 2$, the gradient vector of the quadratic form is nonzero), we can lift this to a vector $v \in L$ with $v \cdot v = 0$. Consider

$$L_v = \mathbf{Z}_p \cdot \frac{1}{p} v + \{w \in L : w \cdot v \equiv 0 \pmod p\}.$$

The claim is that L_v is a p-neighbour of L. To show that it has rank n, note that $L_v \subseteq (1/p)L$ and $pL \subseteq L_v$, giving us $\mathbf{Q}_p^n \subseteq L_v \otimes \mathbf{Q}_p \subseteq \mathbf{Q}_p^n$. Next, consider the map $L_v \to \mathbf{Z}/p\mathbf{Z}$ sending $(a/p)v + w$ to $a \bmod p$. It is certainly injective and its kernel is $L \cap L_v$. It remains to show that L_v is unimodular, which takes a bit of work. Since v is an isotropic vector in a unimodular lattice L, we can find a vector u with $u \cdot v = 0$ such that $\mathbf{Q}_p u \mathbin{\widehat{\oplus}} \mathbf{Q}_p v$ is a hyperbolic plane. Let $\langle u, v\rangle$ denote the span of u and v in the lattice L, and let $\langle u, v\rangle_L^\perp$ denote its complement with respect to L. We have

$$L = \langle u, v\rangle \mathbin{\widehat{\oplus}} \langle u, v\rangle_L^\perp,$$

where since both L and $\langle u, v\rangle$ are unimodular, we conclude that $\langle u, v\rangle_L^\perp$ is. Note that

$$L_v = \left\langle pu, \frac{v}{p} \right\rangle \mathbin{\widehat{\oplus}} \left\langle pu, \frac{v}{p} \right\rangle_{L_v}^\perp.$$

Since $(v/p) \cdot (v/p) = 0 = (pu) \cdot (pu)$ and $(v/p) \cdot (pu) = 1$, the first summand is unimodular. It thus remains to prove that the second summand is. We shall in fact show that $\langle u, v\rangle_L^\perp = \langle v/p, pu\rangle_{L_v}^\perp$. Take $w \in L$ such that $w \cdot v = w \cdot u = 0$. Then $w \in L_v$ and $w \cdot (v/p) = w \cdot pu = 0$. On the other hand, if $w \in L_v$ with $w \cdot (v/p) = w \cdot pu = 0$, then writing $w = (a/p)v + x$ for some $x \in L$, we can write $x = \lambda v + \mu u + y$ where $y \in \langle u, v\rangle_L^\perp$, by the decomposition of L we found earlier. We know that $w \cdot v = p(w \cdot v/p) = 0$ and $w \cdot u = (1/p) w \cdot (pu) = 0$, so w is actually equal to y above, and thus is in L.

We have now shown that we can write

$$L = \langle u_1, v_1\rangle \mathbin{\widehat{\oplus}} \langle u_1, v_1\rangle_L^\perp = \langle u_2, v_2\rangle \mathbin{\widehat{\oplus}} \langle u_2, v_2\rangle_L^\perp$$

where

$$L_1 = \left\langle pu_1, \frac{v_1}{p} \right\rangle \mathbin{\widehat{\oplus}} \left\langle pu_1, \frac{v_1}{p} \right\rangle_{L_v}^\perp$$

and

$$L_2 = \left\langle pu_2, \frac{v_2}{p} \right\rangle \mathbin{\widehat{\oplus}} \left\langle pu_2, \frac{v_2}{p} \right\rangle_{L_v}^\perp.$$

The claim is that the map $g \in G(\mathbf{Q}_p)$ sending $u_1 \mapsto u_2$ and $v_1 \mapsto v_2$ fixes L and sends L_1 to L_2. It is clear that $\langle u_1, v_1\rangle \cong \langle u_2, v_2\rangle = g\langle u_1, v_1\rangle$. Then by Witt's cancellation theorem over $\mathbf{Z}_p$, we have $\langle u_1, v_1\rangle_L^\perp \cong \langle u_2, v_2\rangle_L^\perp = g\langle u_1, v_1\rangle_L^\perp$ as well, which completes the proof that $gL_1 = L_2$. (We proved Witt's cancellation theorem in class for fields but not lattices in general. However, it holds for lattices over $\mathbf{Z}_p$ where p is odd, which can be seen by reducing the lattice modulo p and using the cancellation theorem for $\mathbf{F}_p$; this was proved by B. W. Jones in 1942.) ▮

Symplectic space and the Heisenberg group. A *symplectic space* is a vector space V over a field k endowed with a bilinear form $\langle\cdot,\cdot\rangle : V \times V \to k$, which is alternating in that $\langle v, w\rangle = -\langle w, v\rangle$ for all $v, w \in V$ and which is nondegenerate, i.e., $\langle u, v\rangle = 0$ for all $v \in V$ if and only if $u = 0$. A key example is taking $W = k^2$, with

$$\big\langle (a_1, b_1), (a_2, b_2)\big\rangle = a_1b_2 - a_2b_1.$$

The *Heisenberg group* of a symplectic space W is the set $k \times W$ endowed with the group law

$$(t_1, w_1)(t_2, w_2) = \big(t_1 + t_2 + \langle w_1, w_2\rangle, w_1 + w_2\big).$$

Of course, in the case that W is k^2, this boils down to the group law

$$(t_1, v_1, w_1)(t_2, v_2, w_2) = (t_1 + t_2 + v_1w_2 - v_2w_1, v_1 + v_2, w_1 + w_2)$$

on triples in k^3.

Exercise 14. *Write down the character table of the Heisenberg group $H(W)$ where W is the two-dimensional symplectic space over the field with p elements.*

Solution. There are p elements in the centre of $H(W)$, namely the elements $(t, 0, 0)$ for $t \in k$, so there are p conjugacy classes $\big\{(t, 0, 0)\big\}$ of one element each. The other conjugacy classes are of the form

$$\big\{(t, v_1, v_2) : t \in k\big\}$$

for $(v_1, v_2) \neq (0, 0)$; there are $p^2 - 1$ of these classes, and each of them contains p elements, so we have accounted for all $p + p(p^2 - 1) = p^2$ elements of $H(W)$. So there are $p^2 + p - 1$ characters as well. We shall show that the character table is the following:

Quantity	Dimension	Indexed by	$\big\{(t,0,0)\big\} : t \in k$	$\big\{(*, v, w)\big\} : (v, w) \neq (0, 0)$
p^2	1	$(m, n) \in k^2$	1	${\zeta_p}^{mv+nw}$
$p - 1$	p	$n \in k \setminus \{0\}$	$p{\zeta_p}^{nt}$	0

Let ζ_p be a primitive pth root of unity. There are p^2 representations of degree 1, indexed by $(m, n) \in k^2$, each mapping $(t, v, w) \mapsto {\zeta_p}^{mv+nw}$. For the other $p - 1$ representations, note that there are $p - 1$ nontrivial characters $\psi_n : k \to \mathbf{C}$, given by $\psi_n(t) = {\zeta_p}^{nt}$, where $n \in k \setminus \{0\}$. Each of these gives an action of $H(W)$ on $\mathcal{S}(V)$, since for $f \in \mathcal{S}(V)$, we can let

$$((t, 0, 0) * f)(x) = \psi_n(t)f(x) \qquad \text{and} \qquad ((0, v, w) * f)(x) = \psi_n(-2v \cdot x)f(x + w),$$

It remains to find the trace of these representations on the conjugacy classes. To do so, we take as a basis for $\mathcal{S}(W)$ the p delta functions

$$\delta_y(x) = \begin{cases} 1, & \text{if } x = y; \\ 0, & \text{otherwise} \end{cases}$$

for $y \in V$. In the case where an element of the form $(t, 0, 0)$ acts on the space, each δ_y is taken to $\psi_n(t)\delta_y$, so the matrix has $\psi_n(t)$ down the main diagonal and the trace is $p\psi_n(t) = p{\zeta_p}^{nt}$.

For the conjugacy class $\{(*, v, w)\}$, we shall show that the trace is zero. These elements of $H(W)$ send δ_y to the function $x \mapsto \psi_n(-2v\cdot x)\delta_y(w+x) = \psi_n(-2v\cdot x)\delta_{y-w}$. This means that each row of this transformations's matrix has exactly one nonzero entry, but it cannot be on the main diagonal, having been shifted cyclically by w places. Thus the trace is zero. If $w = 0$, then all of the nonzero entries are still on the main diagonal, but then the trace becomes

$$\sum_{x\in V} \psi_n(-2v \cdot x) = \sum_{x\in V} \psi_n(x) = 0,$$

by Lemma Z and the nondegeneracy of the dot product on $\mathbf{F}_p$. ▮

References

Fred Diamond and Jerry Shurman, *A First Course in Modular Forms* (New York: Springer-Verlag, 2005).

Philippe Gille and Tamás Szamuely, *Central Simple Algebras and Galois Cohomology* (New York: Cambridge University Press, 2006).

Burton Wadsworth Jones, “An extension of a theorem of Witt,” *Bulletin of the American Mathematical Society* **48** (1942), 133–142.

Jean-Pierre Serre, *A Course in Arithmetic* (New York: Springer-Verlag, 1973).

Jean-Pierre Serre, *Linear representations of finite groups* (New York: Springer-Verlag, 1977).

Masaaki Yoshida, *Hypergeometric Functions, My Love* (Wiesbaden: Vieweg + Teubner Verlag, 1997).